JOURNAL OF NUMBER THEORY 10, 10–15 (1978)

The Quadratic Form x^2-2py^2

HORST VON LIENEN

Institut B für Mathematik, Technische Universität, 33 Braunschweig, Germany

Communicated by H. Zassenhaus

Received December 10, 1973

Using known properties of continued fractions, we give a very simple and elementary proof of the theorem of Epstein and Rédei on the impossibility in a certain case of representing -1 by the quadratic form $x^2 - 2py^2$. Two of our theorems, which concern the representation of a^2 and $-2a^2$, serve to extend our method to an unknown case in which -1 is not representable.

1. GENERAL VIEW

Let $2p = r^2 + s^2$ where p is a prime $\equiv 1 \bmod 4$ and r and s are integers. In the table

s	$\equiv \pm 3 \bmod 8$	$\equiv \pm 7 \bmod 16$	$\equiv \pm 1 \bmod 16$
$\equiv \pm 3 \bmod 8$	+	−	−
$\equiv \pm 7 \bmod 16$	−	±	−
$\equiv \pm 1 \bmod 16$	−	−	±

(−) will mean that the equation $x^2 - 2py^2 = -1$ has a solution in integers x and y, (+) that no such solution exists, and (±) that cases of both types occur. In the following the rectangles of the table are numbered from left to right. The proof for the second and third rectangles can be found in Dirichlet [2, pp. 225–226], since $p \equiv 5 \bmod 8$ in these cases. Pall solved the case of rectangle 6 in [4, Theorem 3]. (We correct Pall's theorem by putting $x_2 \equiv \pm 1 \bmod 8$ instead of $x_2 \equiv 1 \bmod 8$.) This case can also be derived from Dirichlet [2, p. 227], since $p = ((r+s)/2)^2 + ((r-s)/2)^2$, and the even fraction is always $\equiv 4 \bmod 8$, so that $2^{(p-1)/4} \equiv -1 \bmod p$.

0022-314X/78/0101–0010$02.00/0

The first rectangle is the theorem of Epstein [3] and Rédei [6]. It is also contained in Pall's theorem 3 [4] when $r \equiv \pm s \bmod 16$ (and therefore $p \equiv 9 \bmod 16$), or otherwise in Pall's Theorem 4. Another simple proof is given in Theorem 3 of this paper. For rectangle 5 we prove in Theorem 4 that the sign is $(+)$ when r is a square and $s \geqslant \frac{4}{3}r$. Numerical calculations suggest that the restriction on s can be omitted, but one finds that the last rectangle is $(\pm)$ even in case r is a square.

In trying to carry over recent results of Brown [1] concerning an odd prime to the case $q = 2$, we find an equivalent property in the cases of rectangles 2 and 3: If $(2 \mid p) = -1$, then -1 is represented by the quadratic form. In all other cases, we must add congruence relations to the power residue criteria: $(p \mid 2)_4 = 1$ is always fulfilled, and if $(2 \mid p)_4 = -1$, -1 is represented in the case of rectangle 6, 2 in the case of rectangle 1. Assuming $(2 \mid p)_4 = 1$, one finds -2 represented in rectangle 1, -1 or 2 or -2 in the other cases on the diagonal, with the exception of -1 in the center rectangle when r is a square.

2. Theorems on Special Representations

THEOREM 1. *Let p be an odd prime. If the quadratic form $x^2 - 2py^2$ represents the odd integer a^2 with $(x, y) = 1$, it also represents one of the integers a, $-a$, $2a$, or $-2a$.*

Proof. Let us assume that in

$$x^2 - a^2 = 2py^2 \tag{1}$$

p divides $x - a$. Then there exists an integer k with

$$x - a = kp. \tag{2}$$

Inserting (2) in (1), we get $kp(kp + 2a) = 2py^2$ or

$$k^2p + 2ak = 2y^2. \tag{3}$$

When q is an odd prime divisor of k, q cannot divide a, since otherwise we obtain $q \mid x$ from (2) and $q^2 \mid 2py^2$ from (1), which makes $q \mid y$ and $q \mid (x, y)$ in contradiction to the assumptions. If α is maximal in $q^\alpha \mid k$, we find $q^\alpha \mid y^2$ in (3). Let α be odd. Then the division by q^α in (3) would leave the first and third term divisible by q, not the second. Therefore α is even. Assuming β maximal in $2^\beta \mid k$, we have $\beta \geqslant 1$ since x and a in (2) are odd, hence $2\beta \geqslant \beta + 1$ and in (3) $2^{\beta+1} \mid 2y^2$ or $2^\beta \mid y^2$. If $\beta > 1$, we conclude as before

that β is even. Then k is a square containing a factor 4, say $k = 4t^2$. Otherwise $k = 2t^2$.

In the first case (2) can be written $(x - a)/2 = 2pt^2$, and we obtain from (1)

$$\frac{x + a}{2} = \frac{py^2/2}{2pt^2} = \frac{y^2}{4t^2}.$$

Because this is an integer, it is a square, say u^2. Now

$$u^2 - 2pt^2 = \frac{x + a}{2} - \frac{x - a}{2} = a$$

is a representation of a by the given quadratic form. If $k = 2t^2$, we divide (1) by (2) and obtain $x + a = y^2/t^2 = u^2$, hence

$$u^2 - 2pt = (x + a) - (x - a) = 2a.$$

The assumption of $x + a = kp$ for (2) leads to a change of sign in the following formulas, but again $k = 4t^2$ or $k = 2t^2$. Defining u^2 as $(x - a)/2$ or $x - a$, we have $u^2 - 2pt^2 = (x - a)/2 - (x + a)/2 = -a$ or $u^2 - 2pt^2 = (x - a) - (x + a) = -2a$, which completes the proof.

THEOREM 2. *When p is a prime and $2p = a^4 + b^2$ with both a^2 and b congruent to 7 or 9 mod 16, the quadratic form $x^2 - 2py^2$ cannot represent $-2a^2$ by integers x and y with x prime to y.*

Proof. Inserting congruences for the squares in

$$x^2 - 2py^2 = -2a^2, \tag{4}$$

one obtains $x^2 \equiv 0, 4$, or $16 \bmod 32$, $2p \equiv 2 \bmod 32$, and $-2a^2 \equiv 14 \bmod 32$. This allows only

$$x^2 \equiv 0 \bmod 32 \quad \text{and} \quad y^2 \equiv 9 \bmod 16, \tag{5}$$

$$\text{or} \quad x^2 \equiv 16 \bmod 32 \quad \text{and} \quad y^2 \equiv 1 \bmod 16. \tag{6}$$

Decompose (4) to

$$(x - by)(x + by) = a^2(a^2y^2 - 2). \tag{7}$$

Since a^2 divides the left-hand side, every prime dividing a is contained in exactly one of the factors $x - by$ or $x + by$ provided we can show that their difference, $2by$, is prime to a. The assumption that $(a, b) = k > 1$ would

lead to $k^2 \mid a^4 + b^2 = 2p$ and p would not be a prime. And if there were a prime l dividing (a, y), we would obtain $l \mid x$ in (4), so that $l \mid (x, y)$. Therefore we can set $(x - by, a^2) = v^2$, $(x + by, a^2) = w^2$, and we have $v^2w^2 = a^2$. Now let

$$x - by = mv^2, \qquad x + by = nw^2. \tag{8}$$

Then from (7) we have $mn = a^2y^2 - 2$.

For every odd prime q that divides mn, one has $(ay)^2 \equiv 2 \bmod q$, hence $q \equiv \pm 1 \bmod 8$. This must also be true for the numbers themselves: $m \equiv \pm 1 \bmod 8$ and $n \equiv \pm 1 \bmod 8$, since mn is odd and the congruence $m = \pm 3 \bmod 8$, for instance, can only exist if m has a prime factor $q' \equiv \pm 3 \bmod 8$; but $q' \mid mn$. According to (5) and (6), the integers $x - by$ and $x + by$ are odd. Therefore (8) implies

$$x - by \equiv \pm 1 \bmod 8, \qquad x + by \equiv \pm 1 \bmod 8. \tag{9}$$

In (5), x is divisible by 8 and $y \equiv \pm 3 \bmod 8$. We obtain further $by \equiv \pm 3 \bmod 8$, hence $x - by \equiv \pm 3 \bmod 8$, which is contrary to (9). Therefore only (6) is left. The right-hand side in (7) is $\equiv 9 \cdot (9 \cdot 1 - 2) \equiv -1 \bmod 16$. Now (9) implies that the factors on the left-hand side of (7) can only be $\equiv 1$ and 15 mod 16 or $\equiv 7$ and 9 mod 16, disregarding the order. The sum $2x$ is always divisible by 16, hence $8 \mid x$, in contradiction to (6). We have thus proved that the Eq. (4) cannot exist.

3. Application to the Representation of -1

The following properties from the theory of continued fractions are used:

(i) Let D be a positive integer, not a square, where $D^{1/2}$ is developed into the simple continued fraction $[b_0, b_1, \ldots, b_{\nu-1}]$, and the inverse of the rest is written $(D^{1/2} + P_\nu)/Q_\nu$. Then the equation $x^2 - Dy^2 = (-1)^\nu Q_\nu$ is solvable with $x = A_{\nu-1}$, $y = B_{\nu-1}$, where $A_{\nu-1}/B_{\nu-1}$ is the $(\nu - 1)$th convergent of the continued fraction of $D^{1/2}$ and $(A_{\nu-1}, B_{\nu-1}) = 1$ (Perron [5, p. 92]).

(ii) If the period of the continued fraction of $D^{1/2}$ has an odd number of terms and $D = r^2 + s^2$, r^2, and s^2 unique, then there exist numbers ν with $P_\nu = r$, $Q_\nu = s$ or $P_\nu = s$, $Q_\nu = r$ (Perron [5, p. 83]). Since $Q_\nu = Q_{\nu-1}$, (i) implies that one of the equations $x^2 - Dy^2 = r$ or $x^2 - Dy^2 = s$ is solvable with positive right-hand side, and $(x, y) = 1$. This coincides with the solvability of the equation $x^2 - Dy^2 = -1$.

THEOREM 3 (Epstein, Rédei). *If p is a prime and $2p = r^2 + s^2$ with r and $s \equiv \pm 3 \bmod 8$, the Diophantine equation $x_0^2 - 2py_0^2 = -1$ is not solvable.*

Proof. The representation of $2p$ as a sum of two squares is unique. Therefore if there were a solution x_0, y_0, one of the equations $x^2 - 2py^2 = r$ or $x^2 - 2py^2 = s$ would also have a solution, according to (ii). That is possible only for x odd, $x^2 \equiv 1 \bmod 8$. Since $2p \equiv 2 \bmod 8$, $2py^2 \equiv 0$ or $2 \bmod 8$, the difference r or s cannot be $\equiv \pm 3 \bmod 8$.

THEOREM 4. *If p is a prime and $2p = a^4 + b^2$ with a^2 and $b \equiv \pm 7 \bmod 16$, the equation $x_0^2 - 2py_0^2 = -1$ cannot have a solution in integers when $b \geqslant \frac{4}{3}a^2$.*

Proof. Assume that $x_0^2 - 2y_0^2 = -1$ is solvable. Then according to the cited properties of continued fractions, either

$$x^2 - 2py^2 = a^2 \qquad \text{or} \qquad x^2 - 2py^2 = b \tag{10}$$

would have a solution. In the first case, we conclude from Theorem 1 that also a representation of $\pm a$ or $\pm 2a$ by the quadratic form exists. The representation of $\pm a$ is impossible, by the proof of Theorem 3. Taking the equation $x_1^2 - 2py_1^2 = \pm 2a$ modulo 16, we have $x_1^2 \equiv 0$ or 4, $2p \equiv 2$, and $\pm 2a \equiv 6$ or 10 mod 16. Hence y_1^2 must be $\equiv 3$ or 5 or 7 mod 8 which is impossible for a square. Therefore only the second equation of (10) is left and we have $P_\nu = a^2$, $Q_\nu = b$, as mentioned above.

If $b = \frac{4}{3}a^2$, one obtains $3 \mid a$, hence $9 \mid 3b$ or $3 \mid b$, and p is not a prime. If $b > \frac{4}{3}a^2$, we deduce $4a^2b < 3b^2$, $a^4 + b^2 < 4b^2 - 4a^2b + a^4$, $(2p)^{1/2} < 2b - a^2$, since $2b - a^2 > a^2 - 2b$, and finally $(a^2 + (2p)^{1/2})/b < 2$. Using the notation of Perron, we have $b_\nu = [(P_\nu + (2p)^{1/2})/Q_\nu] = 1$ and calculate $P_{\nu+1} = b - a^2$, $Q_{\nu+1} = 2a^2$. Since $Q_{\nu-2} = Q_{\nu+1}$, one of the cases would make the equation $x^2 - 2py^2 = -2a^2$ solvable with $(x, y) = 1$. This contradicts Theorem 2.

It is likely that the other possibilities $b_\nu > 1$ or $b < \frac{4}{3}a^2$ do not allow a solution of the equation $x^2 - 2py^2 = -1$, too, but there does not appear to be such an elementary proof in those cases.

REFERENCES

1. E. BROWN, Binary quadratic forms of determinant $-pq$, *J. Number Theory* **4** (1972), 408–410.
2. G. L. DIRICHLET, Einige neue Sätze über unbestimmte Gleichungen, "Werke," Vol. I, pp. 221–236, Kgl. Preuss. Akad. d. Wissensch., Berlin, 1889.

3. P. EPSTEIN, Zur Auflösbarkeit der Gleichung $x^2 - Dy^2 = -1$, *J. Reine Angew. Math.* **171** (1934), 243–252.
4. G. PALL, Discriminantal divisors of binary quadratic forms, *J. Number Theory* **1** (1969), 525–533.
5. O. PERRON, "Die Lehre von den Kettenbrüchen," 3rd ed., I, Teubner, Stuttgart, 1954.
6. L. RÉDEI, Über die Pellsche Gleichung $t^2 - du^2 = -1$, *J. Reine Angew. Math.* **173** (1935), 193–221.